The State Libraries

from previous page...

nology to carry out their daily business, the State Library of Tasmania has put considerable thought and effort into how to avoid the Y2K problem. Over a period of time, the State Library has undertaken a number of measures to ensure a smooth transition at the turn of the millennium.

The State Library identified three main areas of concern:

- hardware used in libraries;
- library systems operating software; and
- administrative software and hardware

The State Library's Library systems support unit has introduced a strategic program of gradually replacing outdated PC hardware with new equipment which is Y2K-compliant.

The current library systems operating software, Dynix, is guaranteed by the supplier as being able to cope with the millennium bug problem. At present the State Library is going through the process of tendering for replacement software. It is anticipated that the new systems software will come into operation within the next twelve months. One of the most important criteria listed in the software specifications is that the new software package must be Y2K-compliant.

The State Library of Tasmania is a division of the Department of Education, Community and Cultural Development (DECCD). The DECCD has its own Informational Technology Branch which provides department wide solutions to information technology challenges and is responsible for information technology infrastructure for the entire Department. One of the Branch's project teams has been working on the Y2K problem for some time, with a specific focus on administrative software and equipment.

The State Library is confident that it has done everything that can reasonably be expected in the way of preparation for the so-called 'millennium bug'.

Cathy Doe, State Library of Tasmania

For whom the bell tolls

Brendan Scott, Gilbert & Tobin

Time: Wednesday 19 January 2000. *Place:* X Holdings — a major repository of bibliographic and holdings data within Australia. Most of the library systems have had relatively low activity over the Christmas period, but university library systems are beginning to generate more traffic. Since Tuesday morning, the X help desk has been receiving queries about intermittent, but spurious, search results and has been trying to track down the problem. X calls on its IT suppliers for maintenance troubleshooting.

Over the following days, the IT supplier discovers the source of the problem — the data has been corrupted, probably by errors in the backup/restore process. It appears that the corruption has resulted from the interaction of the IT supplier's system, X's operating system and the interface used by a number of smaller libraries.

The problem is relatively easy to solve — to restore the integrity of the database involves rolling back a number of weeks and reloading data. It is mid-February before the database has been restored. X has been facing fierce competition from overseas institutions and, as a result of the problems, one major client switches allegiances. Further, X becomes the subject of adverse parliamentary and media comment. It takes many months of crisis management at a public relations level to resolve the problem.

What this scenario attempts to illustrate is that the library community relies on mutual co-operation to operate and there is a broad spread of potential defendants in the event something goes wrong. X may have actions against a number of possible defendants — including the small libraries with the non-compliant interface, the IT supplier, the IT suppliers to the small libraries, the operating system suppliers, and any consultants who have told any of those parties that the system will be Y2K compliant.

Further, there may be questions raised about the management of X. For example, given the amount of publicity surrounding the Y2K problem, they cannot claim that they were unaware of a problem. If X is a public body, it may therefore have failed to discharge its obligations under its governing legislation. Alternatively, if X is a private company the directors may be in breach of their duty to act in the best interests of the company. In both cases, X's officers at a management level may be exposed to both civil and criminal sanctions.

If this is not enough, X will also face the realisation that even if it has good claims against one or more defendants, recovering that money will involve large, technically difficult and, hence, costly litigation. Further, some of the relevant parties may be resident outside of Australia. Some jurisdictions are considering passing legislation limiting companies' liability for Y2K problems (for example, the United States).

One aspect of the Y2K problem which sets it apart from most other legal problems, is that the problem, and its likely time of occurrence, are known. The most logical process now therefore is to develop and implement a risk management strategy to anticipate the risk. Such a strategy should not only seek to prevent the occurrence of problems, but also set in place a means of managing the risk should it eventuate.

It remains to be seen whether the Y2K problem will cause a major or minor disruption to business. What we do know is that the risk exists. We also know that, to a court, to remain ignorant of it will seem more like negligence than bliss. ■